Biotech
Business
Federal
Legal
Managed Care
Pharmaceutical
Research
Special Report
State/Local
Technology
Trends
All Stories
Archives

Magazine
November 2002

Online News
FREE daily and weekly emails
Research
Health Plans
Market Overviews
HealthFax

NEWS FEATURES

HIPAA: Just Good eBiz

To Ensure Practical and Strategic Value, Acquire Broad-Based HIPAA Application Solutions

By Michael Doscher and Mary Staley, for HealthLeaders News, Nov. 6, 2002

Many healthcare organizations are making a strong effort to become compliant with the various requirements of the Health Insurance Portability and Accountability Act of 1996. In the meantime, they have to contend with a number of initiatives, many of which may have HIPAA implications.

Many covered entities, committed to the tenets of HIPAA administrative simplification, are seeking a standards-based health information management solution from the existing offerings of integrated clinical and financial packages. These organizations have an opportunity to both support HIPAA compliance and further their business strategies.

When selecting a system, organizations must keep HIPAA compliance in mind to ensure that applications support e-commerce functions, provide compliant information security, and facilitate support of patient privacy. Some vendors claim to be 'HIPAA compliant.' Just what does that mean? Vendors will have different perspectives of what constitutes HIPAA compliance, so buyers must beware.

Applications intended to support any of the standard HIPAA electronic transactions must contain the appropriate transaction data elements. Furthermore, customers should expect vendors to offer solutions

E-mail Story
Print Story

FEATURES

Healthcare Marketing
Beyond Experience Marketing: Focusing on Customer Impact. 11-18-2002

Healthcare Marketing
Writing an Effective News Release. 11-13-2002

The Cost of Quality
Six Sigma Case Study Series – River Region Health System Emergency Department. 11-15-2002

HealthLeaders EXTRA!
Disease Management – The Reconciliation Blues. 11-11-2002

RELATED ARTICLES

Strategize Now to Take Advantage of HIPAA Opportunities
7-24-2002

California fax newsletter

Special Reports
HIPAA: Are you Ready?

More reports . . .

Roundtables
SURVIVING MERGERS AND SALES: Managing Change

Archives

Event Listings
Events Calendar

Submit an event

addressing the difference in HIPAA's prescribed X12N code tables versus today's custom code tables. Buyers need to consider the following questions:

.

- Is the solution an application that contains tables with X12N codes and definitions? ·
- Is a clearinghouse solution needed? ·
- Are conversion tables the appropriate solution as the vendor moves the application toward being 'HIPAA compliant'?

Buyers must address these and further questions below when selecting or upgrading an application or integrated system. Their inquiries need to reflect each of the three primary parts of HIPAA - transactions, security and privacy.

HIPAA security questions

The proposed HIPAA Technical Security Services characterize the security questions to consider:

1. Does the application provide for emergency access? If so, is a sample written procedure provided for this application? If provided, this technical service would assist organizations as they develop HIPAA-compliant information security policies and procedures.
2. Does the application require unique user identification? Organizations should expect applications to support this service. If unavailable, they should consider other technical means of support or be willing to take on the risk of not being able to easily perform this key security mechanism.
3. Does the application restrict access using context-based, role-based or other user-based access? HIPAA requires one of those forms of access control. If none are available, the organization must find alternative solutions to restricting access.
4. Does the application enable use of access control encryption? Encryption is an alternative technique to support limiting access.
5. What type of audit trail functionality is available to identify suspicious reading or writing intrusion activity?

Preferably, the organization would identify the specific audit requirements prior to the application selection process.

6. What protocols are used for data communications?
7. Does the application require passwords, PINs, biometric, telephone callback, or token to validate identity of the user? The proposed HIPAA security standards require at least one of these methods for user authentication, with organizational decisions required for the level of entity authentication that would be provided, specifically: network, platform or application level.
8. Does the product utilize automatic logoff? While the application itself may not support this function, consideration should be given to whether it would be needed at the application, platform or network level.
9. What type of technology, such as dial-up modems, is needed to provide vendor support? This question provides insight to likely remote access privacy and security vulnerabilities.

Transaction data elements, code sets and identifiers

The final HIPAA standards on transactions and code sets call for a number of significant application changes. Organizations need to identify not only the expected functions of the application to support business transactions by the HIPAA deadline but also the longer term strategic plans to support a more inclusive EDI environment. For applications that process protected health information (PHI) that will not be used for transaction purposes, it still remains important to consider the attributes of data elements compliant with the industry standard code sets and identifiers.

The following questions should be considered to support the HIPAA standard transactions, code sets and identifiers provisions:

1. Does the application collect Provider Code in a 10-position, numeric field format?
2. Does the application collect Employer ID in a 9-position, numeric field format?
3. Does the application support current procedure and

diagnosis code sets (ICD-9, CPT-4, HCPCS)?

4. Does the application support a 5-position, alphanumeric dental code based on CDT?
5. What is the process to adapt the application to major industry code set changes, such as the potential move to ICD-10?
6. Which of the HIPAA standard transactions are supported by the application? Organizations should specifically list the transactions that the application must support with additional information regarding version numbers, release dates and costs. In addition, organizations might consider satisfying more ambitious strategic initiatives requiring more of the HIPAA standard transactions and inquire about their expected availability for planning purposes.
7. Are there any limitations to being able to conduct the transactions the vendor has indicated as compliant? The transactions have some specific data elements related to specific types of care provided or types of organizations, for example, the HIPAA prescribed ASC X12N 837 institutional claim has some specific clinical data elements required for home care claims only. Applications expected to support home care claims must include these data elements.
8. Does the application require the purchase or use of another application or service such as a clearinghouse or interface engine to convert current codes to X12N codes to conduct any of the transactions? Buyers should look for answers regarding the required use of a clearinghouse or an interface engine and consider any additional costs of such processes in the implementation plan.
9. Are the code tables contained in the application X12N compliant? This question should also surface any additional technical support needs or additional costs associated with the implementation.

HIPAA privacy considerations

Organizations should consider the use of technology to comply with the HIPAA privacy standards regarding the ability to define, limit and audit access. The benefits of

technology do not come without potential risk, such as the use of open modem lines frequently used for vendor support. Although appropriate security questions have been addressed as the supporting foundation for privacy compliance, other specific considerations should be addressed with vendors in advance of contract signature to prevent potential privacy risks.

Some questions to pose to potential application vendors include:

1. Does the vendor have access to the live application environment once installed? Obvious issues exist with vendors who access live environments and possibly intend to use an organization's clinical information to enhance an application. This possibility is a real-life example of questionable vendor use of HIPAA defined PHI.
2. What mechanisms are in place to secure and ensure the privacy of our information during vendor support activities? Although this support is somewhat open-ended, organizations should look for responses that include:
    a. Security, privacy and confidentiality training of employees.
    b. Logs of support personnel access to PHI.
    c. The various requirements of a Business Associate Agreement if, in fact, the vendor falls into that category based on PHI access.
3. Can the vendor support the requirements of the HIPAA privacy business associate agreement? If PHI is being accessed to support the buyer's operations, vendors should expect to sign such agreements. Business associate agreements call for processes that would do the following:
    a. Limit further release of PHI by the vendor.
    b. Require the vendor to report privacy incidents and response.
    c. Ensure the appropriate destruction or return of the information upon contract termination.

Organizations should revise the questions based on expected application functions and overall organizational strategy. The intent of HIPAA's Administrative Simplification standards is to foster uniformity in how the healthcare industry conducts business. In doing so, organizations have an opportunity to further support their strategies, including application replacement, upgrade and implementation. Once the questions have been identified, organizations should determine the appropriate categories of responses and place a weight on each to allow for a more objective comparison.

One example of a tool for comparison is pictured below in Diagram 1.

Diagram 1. Sample Application Questionnaire

Question	Vendor Response	HIPAA Section	Compliance Score	Weight	Overall Score
Is a sample written Emergency Access Procedure provided for this application?		Security .308.c.1			

Compliance scores might include:

- Compliant (Indicated by a value of 3) - Meets or exceed expectations
- Work-Around (Indicated by a value of 2) - Does not meet expectations, although a work-around solution is offered
- Non-Compliant (Indicated by a value of 1) - Does not meet required expectations

Suggested weighting includes:

- 1 - Not needed
- 3 - Nice to have
- 5 - Required

For each question, a calculation of the compliance score multiplied by the weight would provide a "quasi" objective overall score. A simple sum of all overall scores would provide the buyer with the ability to compare the vendors' applications or systems.

'HIPAA compliance' is a complicated issue for everyone - covered entities, business associates and vendors alike. Healthcare organizations should keep HIPAA compliance issues in mind now as they pursue strategic information systems initiatives.

Organizations must clearly define the current and future intents and expectations of their core applications in order to ensure a full disclosure of those requirements to vendors during the selection process. The covered entities should not view their HIPAA compliance as simply dependent on the vendor's solution. HIPAA offers instead an organizational opportunity that their vendors must support.

Michael Doscher has more than 25 years senior management and consulting experience with healthcare information technology. He is now assisting clients in planning and implementing their HIPAA compliance requirements. Contact Mike at Mike.Doscher@healthlinkinc.com

In May 2002, the American Medical Association published his book, **HIPAA: A Short and Long Term Perspective for Healthcare.** For more information, click here

Mary Staley is a Vice President for Healthlink's HIPAA practice. She may be contacted at Mary.Staley @healthlinkinc.com.

SEND TO FRIEND | POST OPINION

PREVIOUS

HIPAA: Just Good eBiz

To Ensure Practical and Strategic Value, Acquire Broad-Based HIPAA Application Solutions

By Michael Doscher and Mary Staley, for HealthLeaders News, Nov. 6, 2002

Strategize Now to Take Advantage of HIPAA Opportunities

By Michael Doscher, for HealthLeaders.com, July 24, 2002